

Verify and Identify Packet Loss in the WAN for SD-WAN

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background](#)

[Troubleshoot Process](#)

[Overview Process](#)

[Mark the Desired traffic with DSCP](#)

[Capture the Traffic with the Embedded Capture](#)

[Analysis through Wireshark](#)

[Filter the Desired Traffic by ESP Sequence](#)

[Related Information](#)

Introduction

This document describes how to identify and collect data when traffic has loss across the WAN but no drops are seen on the SD-WAN Edge.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Software-Defined Wide Area Network (SD-WAN)
- Embedded Packet Capture or vManage Packet Capture
- Wireshark
- Microsoft Excel

Components Used

The information in this document is based on these software and hardware versions:

- C8000V version 17.03.04
- vManage version 20.3.4
- Wireshark version 2.6.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background

In order to assist with this challenge, the steps described in this doc shows how to mark specific traffic with Differentiated Services Code Point (DSCP) to help to identify the desired packets. DSCP can be used to identify the traffic since this value is copied from the inner packet header to the IPsec header. Once the desired packets are identified, it shows how to match the traffic across two WAN captures to ensure traffic made it from source to destination.

Two single router sites are used to demonstrate this troubleshoot technique. In this case, ICMP traffic from 10.0.0.10 to 10.0.2.10 in the form of 100 pings as shown in the image. There is no loss in this example but this same troubleshoot technique is used in the case where there is a loss to identify it.



Troubleshoot Process

Overview Process

1. For the traffic traced across the WAN, an Access List (ACL) (or centralized policy) is needed to mark traffic with some unused DSCP value. In this example, DSCP 27 is used.
2. Once the traffic is marked, embedded packet capture is used to capture the packets on the transport interface of the source and destination router.

Note: vManage packet capture can also be used although there is a limitation of 5MB of data or 5 minutes of runtime.

1. After the captures are taken, open them in Wireshark to view.
2. The filter is applied in Wireshark to show which packets are desired and then they are compared.
3. Microsoft Excel is used for large captures to ensure accuracy.

Mark the Desired traffic with DSCP

An access-list such as the example is configured on the source router (cEdge1 in this example) and applied on the interface in the SD-WAN portion of the router config as shown.

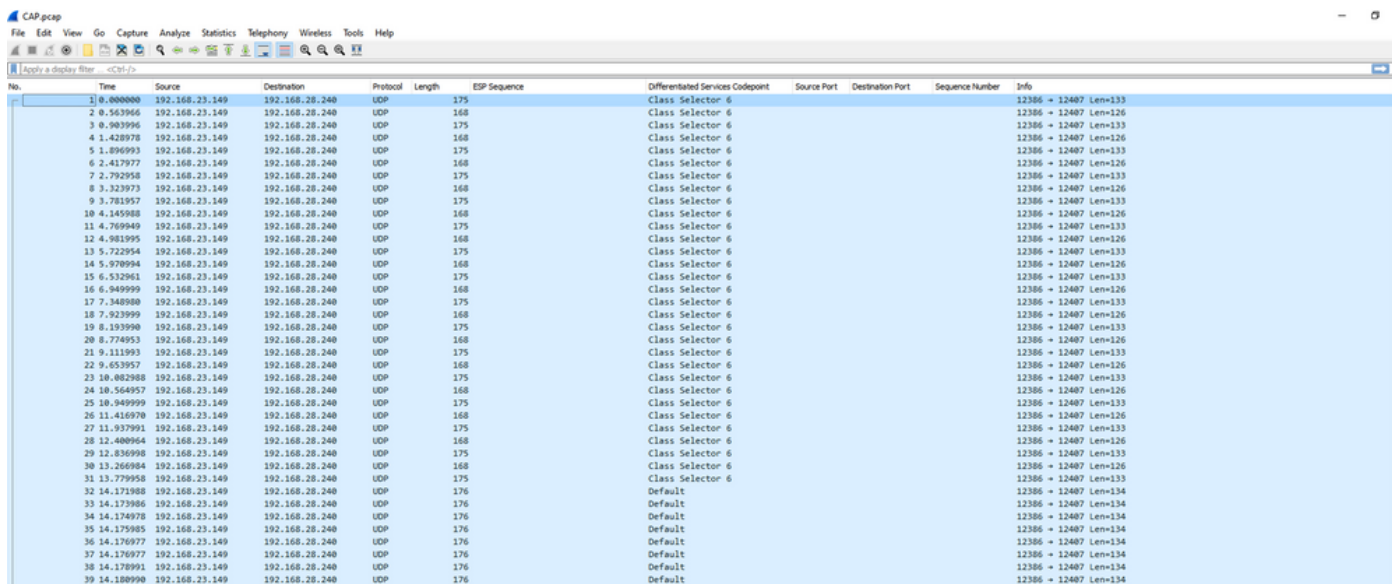
An optional counter is applied to verify that traffic hits the policy as expected. This can be checked

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/4 ms

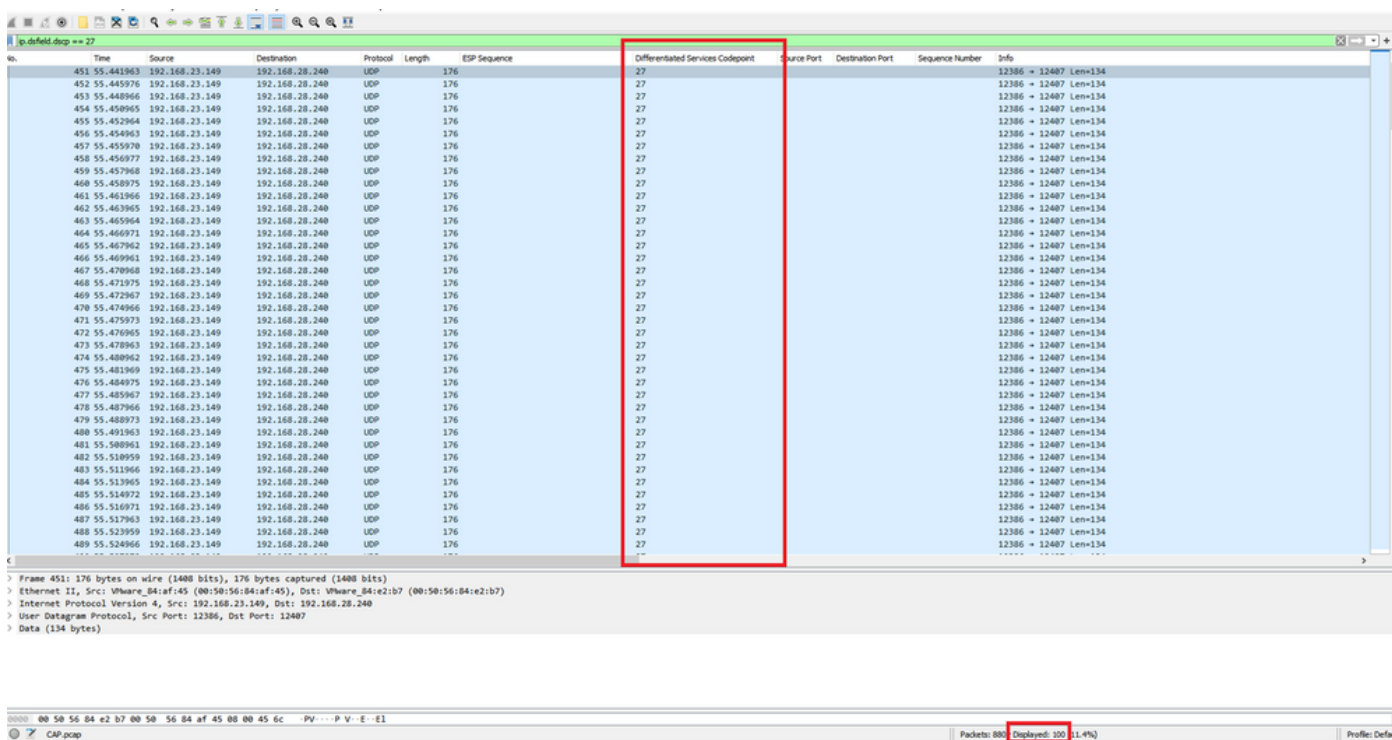
After the captures are stopped and collected from both routers, they need to be opened in Wireshark to view them.

Analysis through Wireshark

Once the cEdge1 capture is opened in Wireshark it is seen that all the traffic is encrypted and it is not easy to decipher which packets are the pings which were sent.



Filter this capture with a display filter `ip.dsfield.dscp == 27`, it is seen that only 100 packets are displayed at the bottom of the screen and it is seen that the DSCP column value all shows 27.



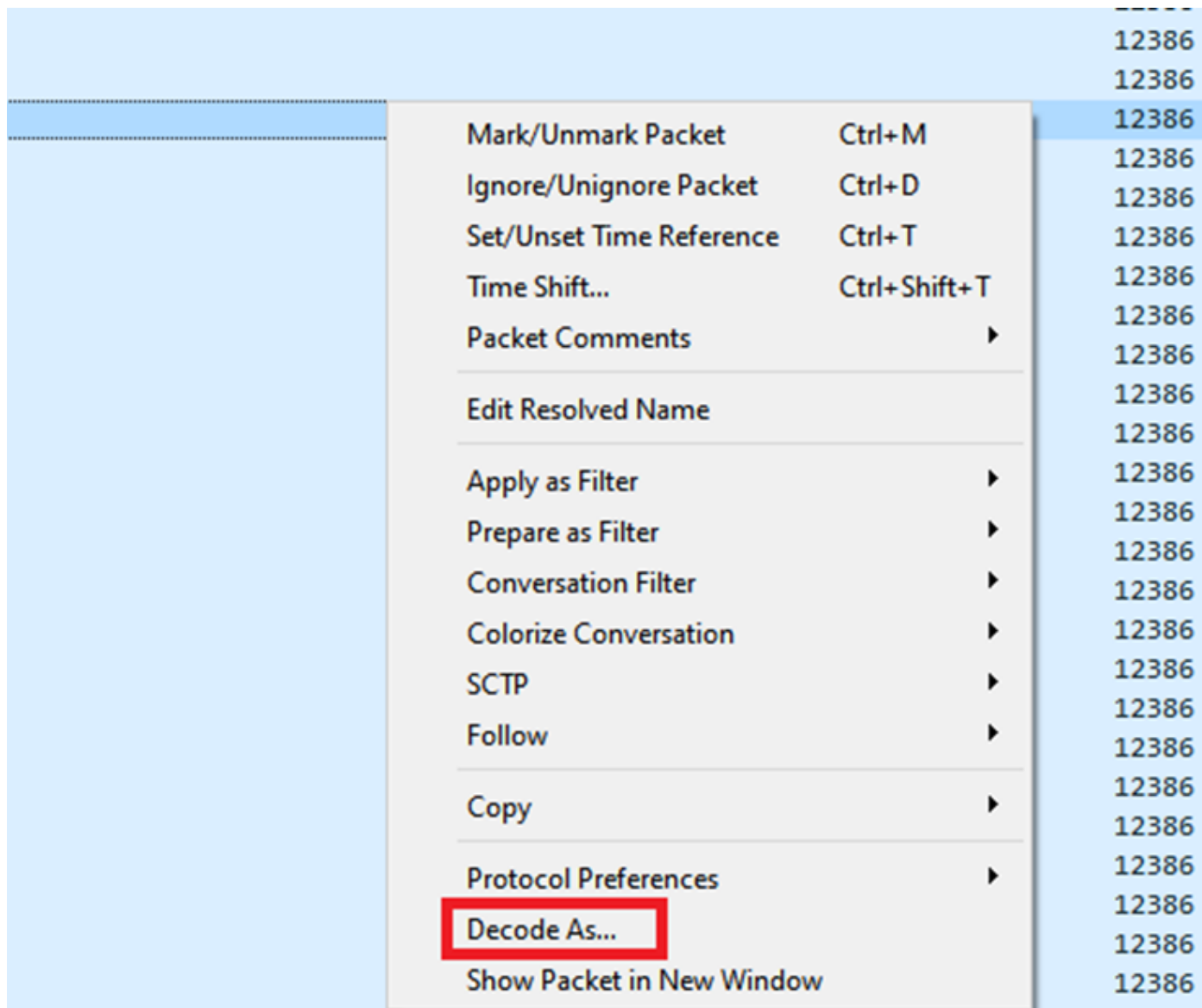
In some cases where DSCP value is maintained across the WAN, the same filter can be used on the destination capture.

In other cases, this is not possible such as a situation where DSCP value is cleared across a public-internet connection.

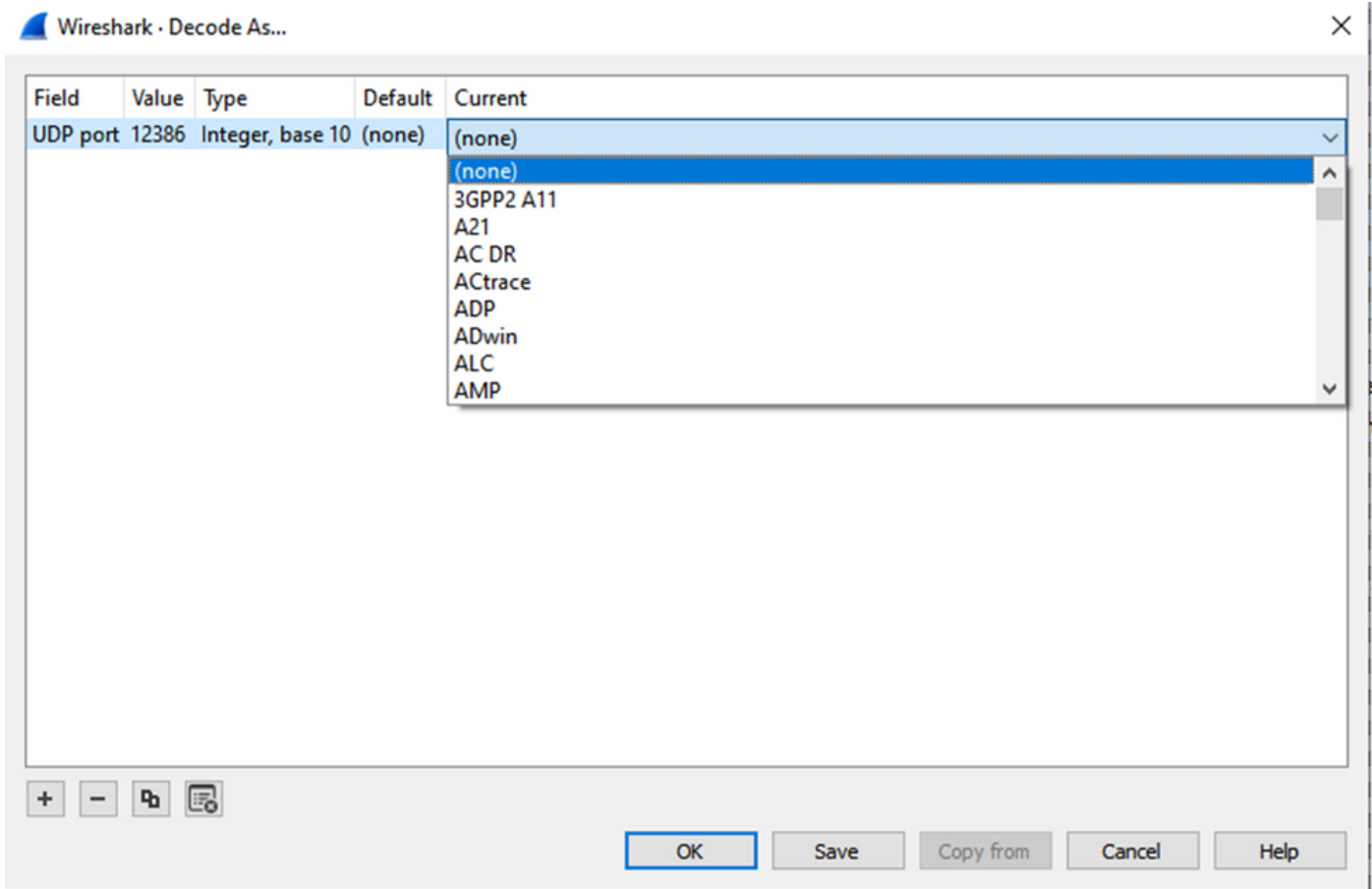
Filter the Desired Traffic by ESP Sequence

In either case, the traffic can be identified with the ESP sequence numbers.

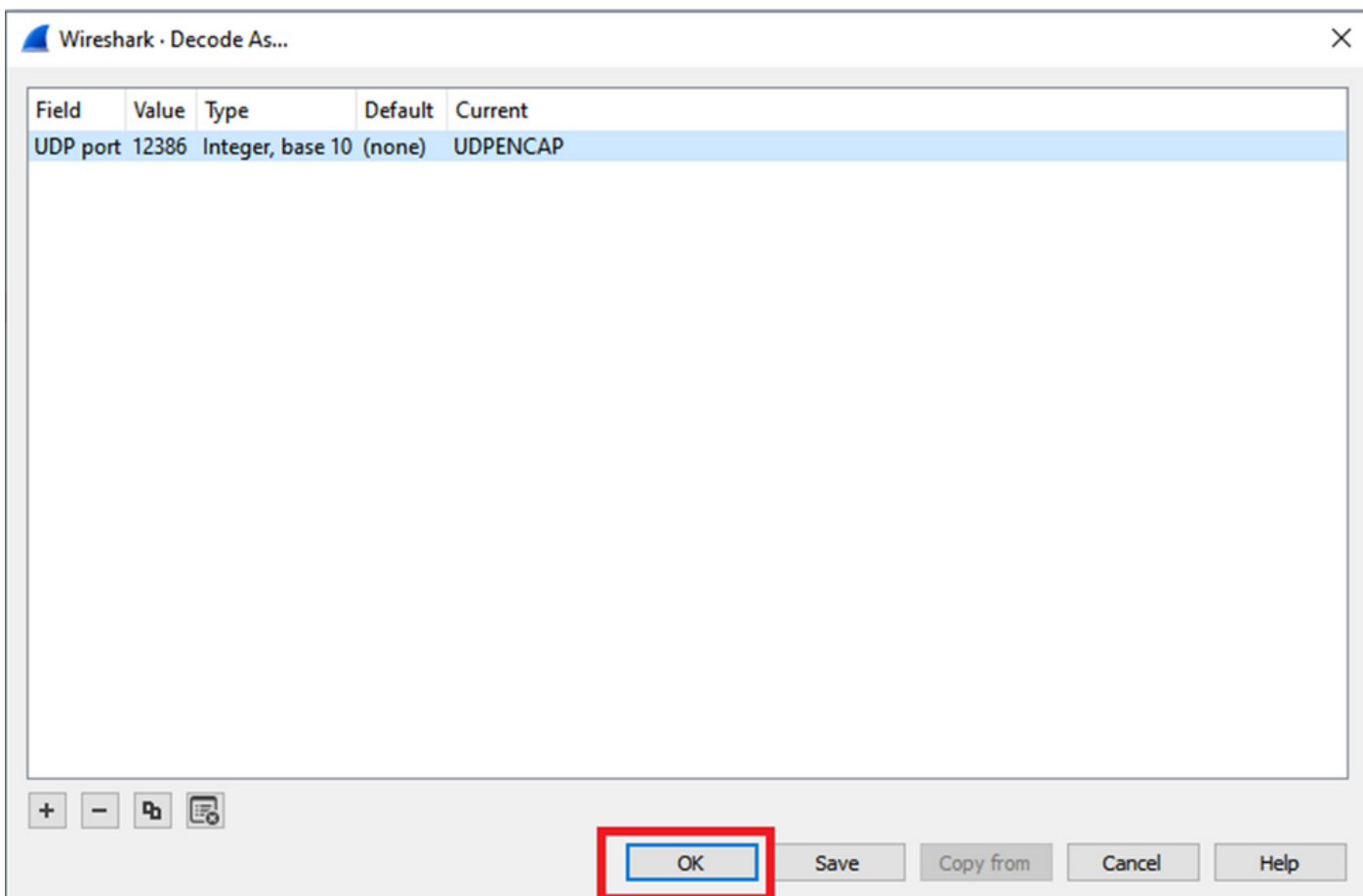
To see the ESP sequence numbers in the packet, right click on the capture and choose **Decode as** as shown.



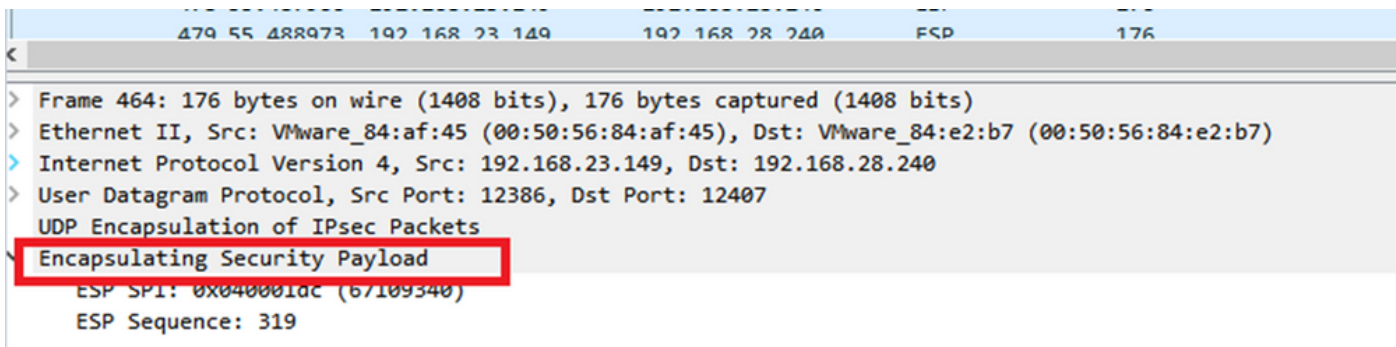
Select the **Current** field dropdown menu and in that field type **UDPENCAP** or select it from the dropdown.



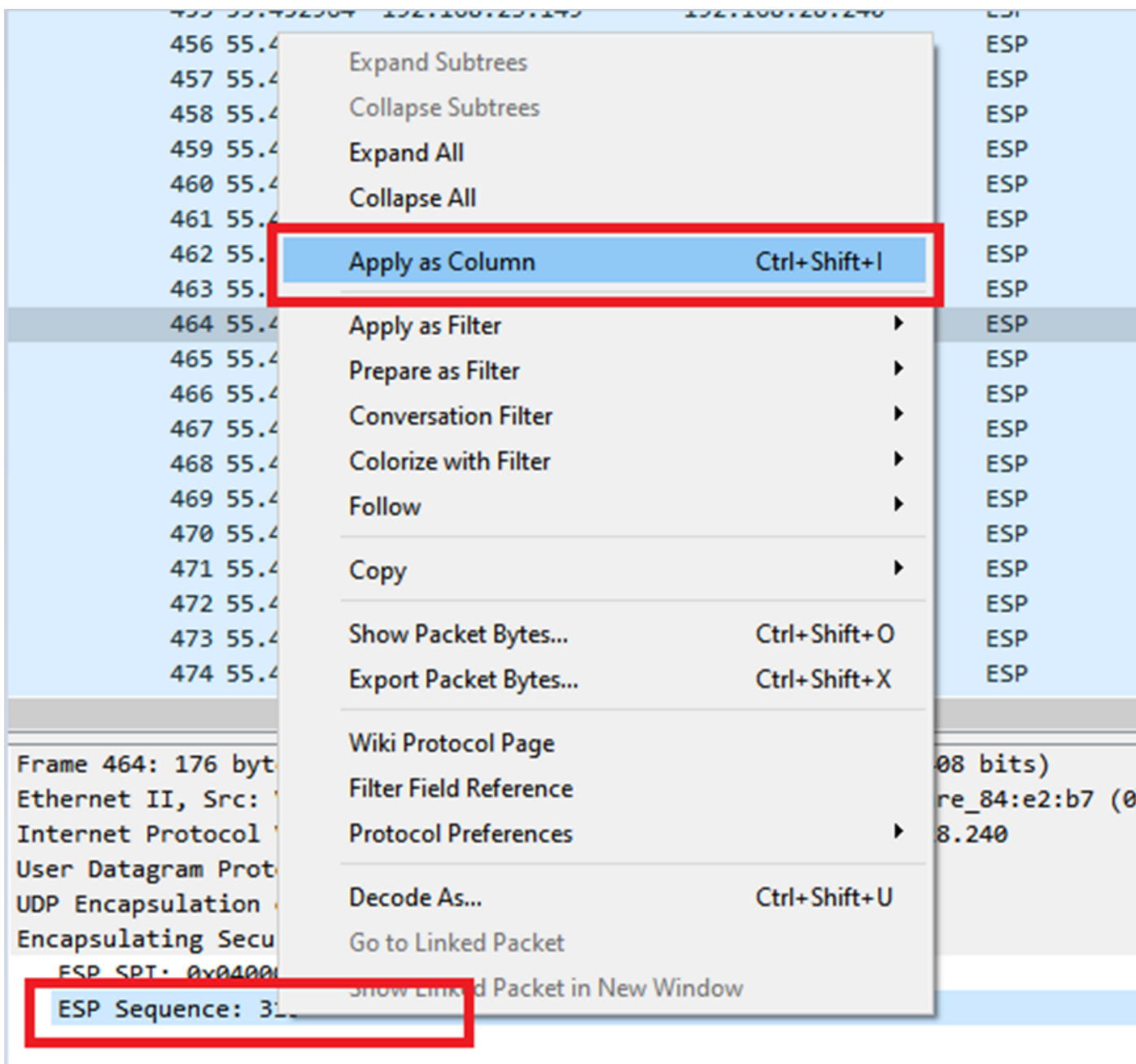
Select the **OK** once this is completed.



Within the Wireshark Packet Details section, expand the **Encapsulating Security Payload** portion of the packet to see **ESP Sequence**.



Right click on **ESP Sequence** and choose **apply as column** so the ESP Sequence can be seen as a column in the Packet List section at the top portion of the Wireshark screen.



Note: The ESP SPI for the packets on cEdge1 is **0x040001dc**. This is used for a filter on the destination capture.

```

> Frame 464: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)
> Ethernet II, Src: VMware_84:af:45 (00:50:56:84:af:45), Dst: VMware_84:e2:b7
> Internet Protocol Version 4, Src: 192.168.23.149, Dst: 192.168.28.240
> User Datagram Protocol, Src Port: 12386, Dst Port: 12407
  UDP Encapsulation of IPsec Packets
  Encapsulating Security Payload
    ESP SPI: 0x040001dc (67109340)
    ESP Sequence: 319
  
```

Open the destination capture, repeat the steps to decode as **UDPENCAP**, and display the ESP Sequence numbers in the packets.

Once the packets display the ESP Sequence number, the ESP SPI from the first capture can be used as a filter on the second capture to display only the traffic within that SPI that matches the desired traffic.

Notice that the packet sequence numbers that match both have DSCP 27 marked.

The image shows two Wireshark windows side-by-side. The left window, titled 'ip.dsfield.dscp == 27', displays a list of packets with columns for Time, Source, Destination, Protocol, Length, and ESP Sequence. The right window, titled 'CAP2.pcap', displays a list of packets with columns for Time, Source, Destination, Protocol, Length, and ESP Sequence. Red boxes highlight the 'DSCP 27' field in the left window and the 'ESP SPI: 0x040001dc' field in the right window. Red lines connect the corresponding packets between the two windows, showing that the same sequence numbers are present in both captures.

This comparison can be done in Wireshark manually or Microsoft Excel can be used to do this comparison.

In order to use Microsoft Excel to compare, it is necessary to slice both captures to contain only packets which are in both captures.

In the source capture, the first relevant packet has ESP sequence 306 and that corresponds to packet number 451.

The screenshot shows a Wireshark window with a filter 'ip.dsfield.dscp == 27'. The packet list is displayed in a table format with the following columns: No., Time, Source, Destination, Protocol, Length, ESP Sequence, and Different. The table contains the following data:

No.	Time	Source	Destination	Protocol	Length	ESP Sequence	Different
451	55.441963	192.168.23.149	192.168.28.240	ESP	176	306 27	
452	55.445976	192.168.23.149	192.168.28.240	ESP	176	307 27	
453	55.448966	192.168.23.149	192.168.28.240	ESP	176	308 27	
454	55.450965	192.168.23.149	192.168.28.240	ESP	176	309 27	
455	55.452964	192.168.23.149	192.168.28.240	ESP	176	310 27	
456	55.454963	192.168.23.149	192.168.28.240	ESP	176	311 27	
457	55.455970	192.168.23.149	192.168.28.240	ESP	176	312 27	
458	55.456977	192.168.23.149	192.168.28.240	ESP	176	313 27	

The last relevant packet in the source capture has ESP sequence 405 and is packet number 550.

548	55.608962	192.168.23.149	192.168.28.240	ESP	176	403	27
549	55.609969	192.168.23.149	192.168.28.240	ESP	176	404	27
550	55.610960	192.168.23.149	192.168.28.240	ESP	176	405	27

In the destination capture, the first relevant packet corresponds to the source capture with ESP Sequence 306 but in this capture is packet 463.

461	60.522028	192.168.23.149	192.168.28.240	ESP	168	407	Class Se
462	60.715026	192.168.23.149	192.168.28.240	ESP	175	408	Class Se
463	60.999008	192.168.23.149	192.168.28.240	ESP	176	306	27
464	61.003006	192.168.23.149	192.168.28.240	ESP	176	307	27

The last relevant packet is also present with ESP Sequence 405 and it is packet 564.

560	61.165052	192.168.23.149	192.168.28.240	ESP	176	405	27
561	61.166043	192.168.23.149	192.168.28.240	ESP	176	404	27
562	61.166043	192.168.23.149	192.168.28.240	ESP	176	405	27
563	61.431029	192.168.23.149	192.168.28.240	ESP	168	409	Class Se
564	61.584021	192.168.23.149	192.168.28.240	ESP	175	410	Class Se

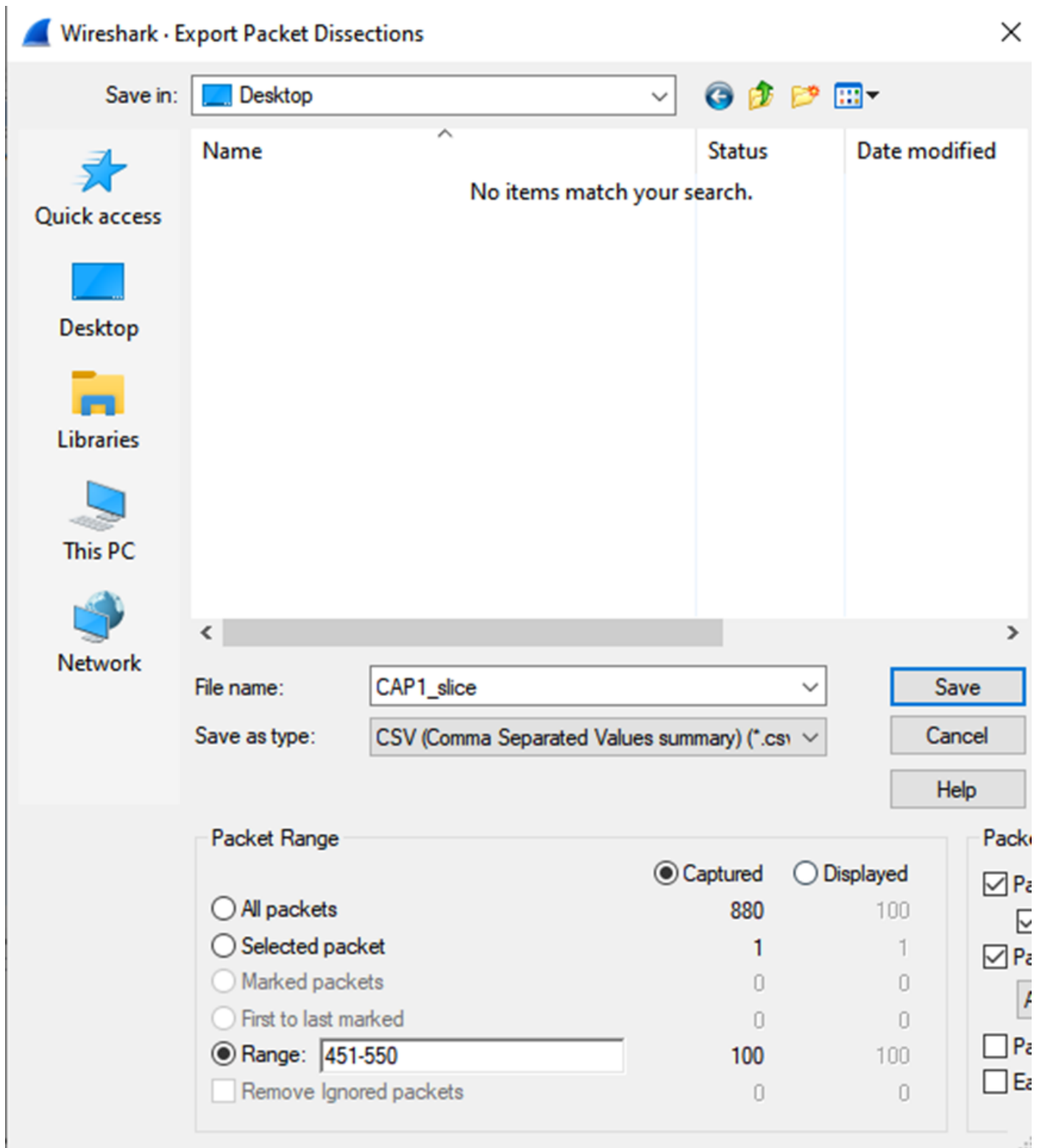
The first capture must now be sliced to include only relevant packets.

Navigate to **File > Export Packet Dissections > As CSV...**

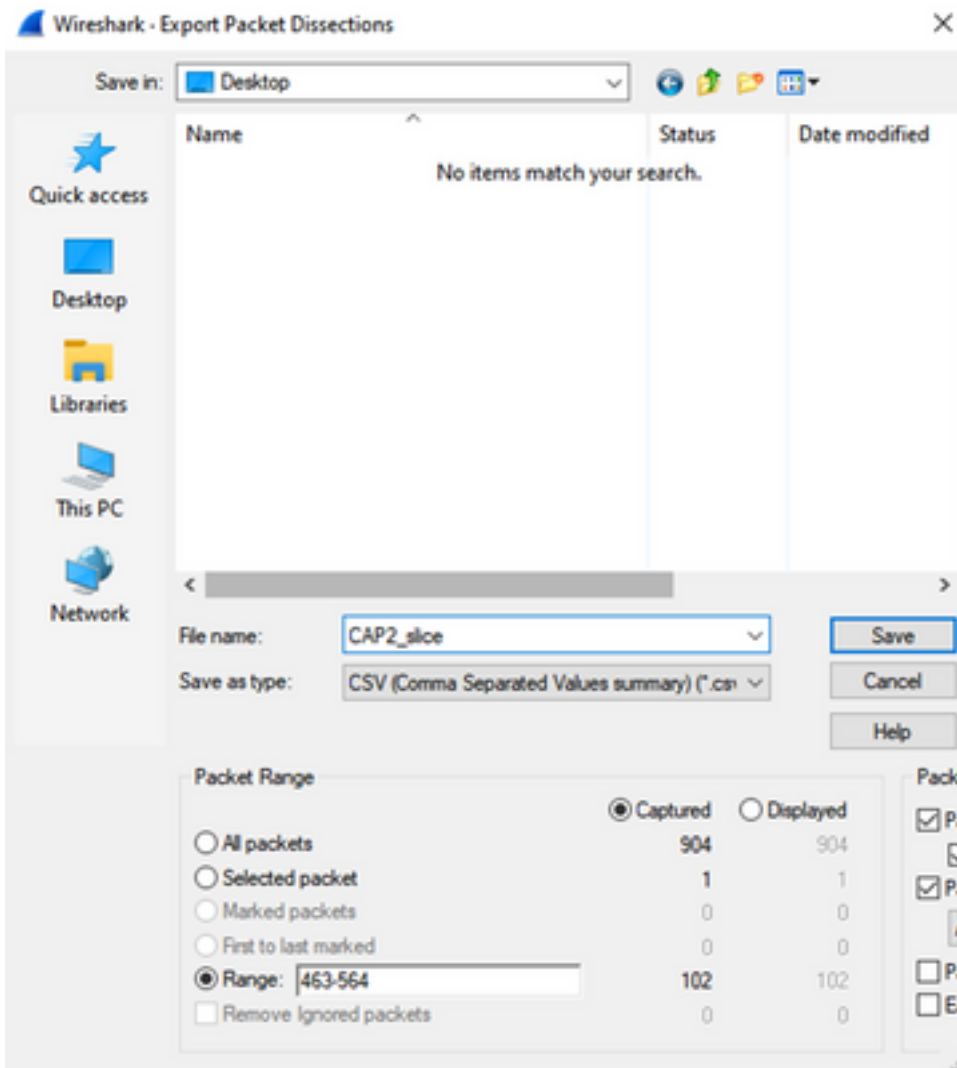
The screenshot shows the Wireshark application window with the 'CAP.pcap' file open. The 'File' menu is open, and the 'Export Packet Dissections' option is selected, which has opened a sub-menu. In this sub-menu, the 'As CSV...' option is highlighted. The background shows a packet list table with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 548) is highlighted in blue. The sub-menu options include 'As Plain Text...', 'As CSV...', 'As "C" Arrays...', 'As PSML XML...', 'As PDML XML...', and 'As JSON...'. The 'As CSV...' option is the one to be selected for the next step.

Select **Captured** and **Range** and in the **Range** field type the range from the first relevant packet to the last relevant packet.

Enter a file name in the **File Name** field and click **Save**.

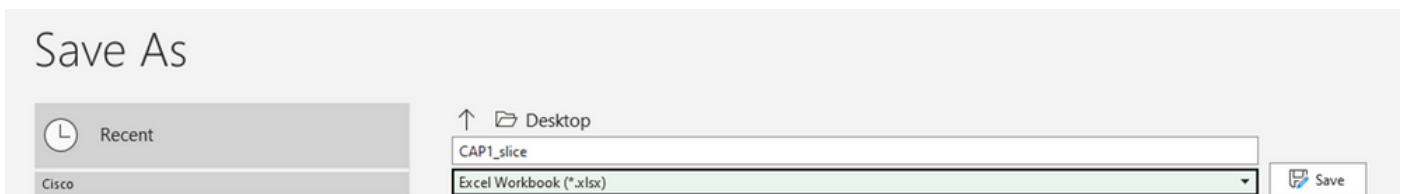


Repeat the same process on capture 2 for the relevant packets.

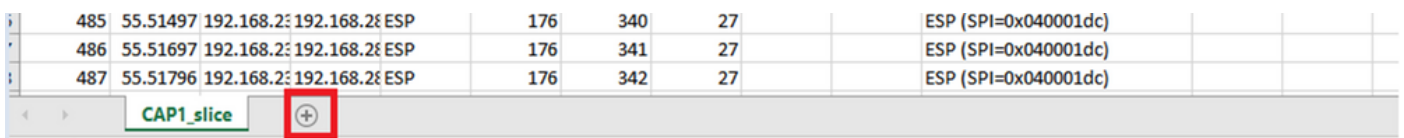


Open both CSV files in Microsoft Excel.

On the source capture **CSV**, save as an **XLSX format**.



At the bottom of the screen, select the **+** symbol to add another sheet. Name it **CAP2_slice**.



Open the **CAP2 CSV** file and press **CTRL + a** to select all and **CTRL + c** to copy it.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	No.	Time	Source	Destinatic	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatic	Info	Sequence	Number
2	463	60.99901	192.168.25	192.168.25	ESP	176	306	27			ESP (SPI=0x040001dc)		
3	464	61.00301	192.168.25	192.168.25	ESP	176	307	27			ESP (SPI=0x040001dc)		
4	465	61.00506	192.168.25	192.168.25	ESP	176	308	27			ESP (SPI=0x040001dc)		
5	466	61.00706	192.168.25	192.168.25	ESP	176	309	27			ESP (SPI=0x040001dc)		
6	467	61.00905	192.168.25	192.168.25	ESP	176	310	27			ESP (SPI=0x040001dc)		
7	468	61.01006	192.168.25	192.168.25	ESP	176	311	27			ESP (SPI=0x040001dc)		
8	469	61.01105	192.168.25	192.168.25	ESP	176	312	27			ESP (SPI=0x040001dc)		
9	470	61.01305	192.168.25	192.168.25	ESP	176	313	27			ESP (SPI=0x040001dc)		
10	471	61.01406	192.168.25	192.168.25	ESP	176	314	27			ESP (SPI=0x040001dc)		
11	472	61.01606	192.168.25	192.168.25	ESP	176	315	27			ESP (SPI=0x040001dc)		
12	473	61.01806	192.168.25	192.168.25	ESP	176	316	27			ESP (SPI=0x040001dc)		
13	474	61.02106	192.168.25	192.168.25	ESP	176	317	27			ESP (SPI=0x040001dc)		
14	475	61.02205	192.168.25	192.168.25	ESP	176	318	27			ESP (SPI=0x040001dc)		
15	476	61.02306	192.168.25	192.168.25	ESP	176	319	27			ESP (SPI=0x040001dc)		
16	477	61.02506	192.168.25	192.168.25	ESP	176	320	27			ESP (SPI=0x040001dc)		
17	478	61.02605	192.168.25	192.168.25	ESP	176	321	27			ESP (SPI=0x040001dc)		

Navigate to the **CAP1_slice.xlsx** file and on the second tab for CAP2_slice, paste (**CTRL + v**) the copied information into the cell **A1**.

Clipboard

Cut Copy Paste Format Painter

Font

Calibri 11 Bold Italic Underline Text Color Background Color

Alignment

Wrap Text Merge & Center

Number

General \$ % .00

A1

	A	B	C	D	E	F	G	H	I	J	K	L	M
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													
21													
22													
23													
24													
25													
26													
27													
28													
29													
30													
31													
32													
33													
34													
35													
36													
37													
38													

1	No.	Time	Source	Destinatic	Protocol	Length	ESP Sequ	Differenti	Source Po	Destinatic	Info	Sequence N
2	463	60.99901	192.168.2	192.168.2	ESP	176	306	27			ESP (SPI=0x040001dc)	
3	464	61.00301	192.168.2	192.168.2	ESP	176	307	27			ESP (SPI=0x040001dc)	
4	465	61.00506	192.168.2	192.168.2	ESP	176	308	27			ESP (SPI=0x040001dc)	
5	466	61.00706	192.168.2	192.168.2	ESP	176	309	27			ESP (SPI=0x040001dc)	
6	467	61.00905	192.168.2	192.168.2	ESP	176	310	27			ESP (SPI=0x040001dc)	
7	468	61.01006	192.168.2	192.168.2	ESP	176	311	27			ESP (SPI=0x040001dc)	
8	469	61.01105	192.168.2	192.168.2	ESP	176	312	27			ESP (SPI=0x040001dc)	
9	470	61.01305	192.168.2	192.168.2	ESP	176	313	27			ESP (SPI=0x040001dc)	
10	471	61.01406	192.168.2	192.168.2	ESP	176	314	27			ESP (SPI=0x040001dc)	
11	472	61.01606	192.168.2	192.168.2	ESP	176	315	27			ESP (SPI=0x040001dc)	
12	473	61.01806	192.168.2	192.168.2	ESP	176	316	27			ESP (SPI=0x040001dc)	
13	474	61.02106	192.168.2	192.168.2	ESP	176	317	27			ESP (SPI=0x040001dc)	
14	475	61.02205	192.168.2	192.168.2	ESP	176	318	27			ESP (SPI=0x040001dc)	
15	476	61.02306	192.168.2	192.168.2	ESP	176	319	27			ESP (SPI=0x040001dc)	
16	477	61.02506	192.168.2	192.168.2	ESP	176	320	27			ESP (SPI=0x040001dc)	
17	478	61.02605	192.168.2	192.168.2	ESP	176	321	27			ESP (SPI=0x040001dc)	
18	479	61.02805	192.168.2	192.168.2	ESP	176	322	27			ESP (SPI=0x040001dc)	
19	480	61.02906	192.168.2	192.168.2	ESP	176	323	27			ESP (SPI=0x040001dc)	
20	481	61.02906	192.168.2	192.168.2	ESP	176	324	27			ESP (SPI=0x040001dc)	
21	482	61.03005	192.168.2	192.168.2	ESP	176	325	27			ESP (SPI=0x040001dc)	
22	483	61.03206	192.168.2	192.168.2	ESP	176	326	27			ESP (SPI=0x040001dc)	
23	484	61.03306	192.168.2	192.168.2	ESP	176	327	27			ESP (SPI=0x040001dc)	
24	485	61.03505	192.168.2	192.168.2	ESP	176	328	27			ESP (SPI=0x040001dc)	
25	486	61.03606	192.168.2	192.168.2	ESP	176	329	27			ESP (SPI=0x040001dc)	
26	487	61.03905	192.168.2	192.168.2	ESP	176	330	27			ESP (SPI=0x040001dc)	
27	488	61.04105	192.168.2	192.168.2	ESP	176	331	27			ESP (SPI=0x040001dc)	
28	489	61.04206	192.168.2	192.168.2	ESP	176	332	27			ESP (SPI=0x040001dc)	
29	490	61.04406	192.168.2	192.168.2	ESP	176	333	27			ESP (SPI=0x040001dc)	
30	491	61.04606	192.168.2	192.168.2	ESP	176	334	27			ESP (SPI=0x040001dc)	
31	492	61.06305	192.168.2	192.168.2	ESP	176	335	27			ESP (SPI=0x040001dc)	
32	493	61.06505	192.168.2	192.168.2	ESP	176	336	27			ESP (SPI=0x040001dc)	
33	494	61.06705	192.168.2	192.168.2	ESP	176	337	27			ESP (SPI=0x040001dc)	
34	495	61.06905	192.168.2	192.168.2	ESP	176	338	27			ESP (SPI=0x040001dc)	
35	496	61.07105	192.168.2	192.168.2	ESP	176	339	27			ESP (SPI=0x040001dc)	
36	497	61.07105	192.168.2	192.168.2	ESP	176	340	27			ESP (SPI=0x040001dc)	
37	498	61.07305	192.168.2	192.168.2	ESP	176	341	27			ESP (SPI=0x040001dc)	

Navigate back to **CAP1_slice** sheet and make a new column called **COMPARE_ESP_SEQUENCE**.

1	No.	Time	Source	Destinatic	Protocol	Length	ESP Sequ	Differenti	Source Po	Destinatic	Info	Sequence Number	COMPARE_ESP_SEQUENCE
2	451	55.44196	192.168.2	192.168.2	ESP	176	306	27			ESP (SPI=0x040001dc)		
3	452	55.44598	192.168.2	192.168.2	ESP	176	307	27			ESP (SPI=0x040001dc)		
4	453	55.44807	192.168.2	192.168.2	ESP	176	308	27			ESP (SPI=0x040001dc)		

As the ESP Sequence number is in Column G, compose a VLOOKUP command as shown to compare the two sheets to ensure that everything in Column G on the source is in Column G on the destination.

=IF(ISNA(VLOOKUP(G2,CAP2_slice!G:G,1,FALSE)),"MISSING","PRESENT")

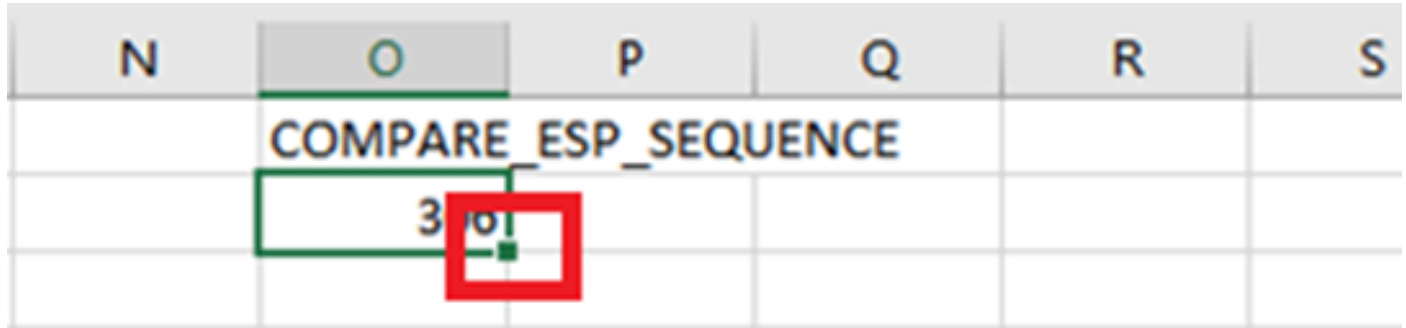
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	
Time	Source	Destinatic	Protocol	Length	ESP Sequ	Differenti	Source Po	Destinatic	Info	Sequence Number			COMPARE	ESP_SEQUENCE									
55.44196	192.168.2	192.168.2	ESP	176	306	27			ESP (SPI=0x040001dc)				=IF(ISNA(VLOOKUP(G2,CAP2_slice!G:G,1,FALSE)),"MISSING","PRESENT")										
55.44598	192.168.2	192.168.2	ESP	176	307	27			ESP (SPI=0x040001dc)														

After Enter is selected the word PRESENT is displayed. This means that the packet with ESP Sequence **306** is present in the second sheet. This is significant because it means that the packet

made it from the source to the destination.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	No.	Time	Source	Destinatic Protocol	Length	ESP Sequ	Differenti	Source Po	Destinatic Info	Sequence Number					COMPARE	ESP_SEQUENCE		
2	451	55.44196	192.168.2.2	192.168.2.2	ESP	176	306	27			ESP (SPI=0x040001dc)				PRESENT			
3	452	55.44598	192.168.2.2	192.168.2.2	ESP	176	307	27			ESP (SPI=0x040001dc)							

Select Column O Row 2 and hover over the bottom right corner of the green box around that cell.

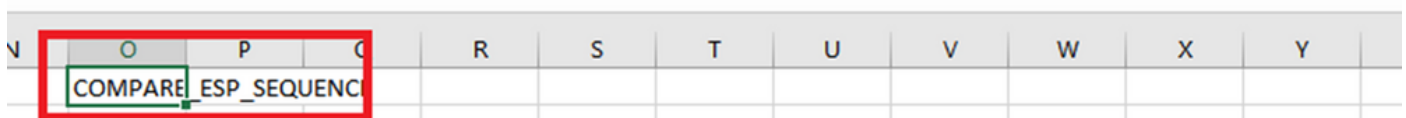
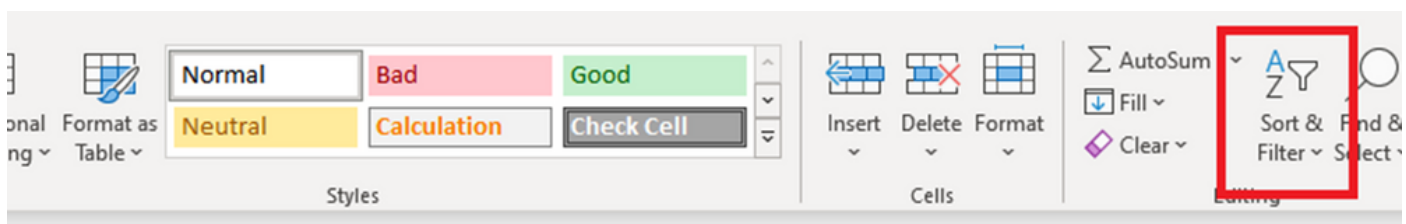


Select and hold, and drag the mouse down to copy this formula to the bottom of the cells which have values.

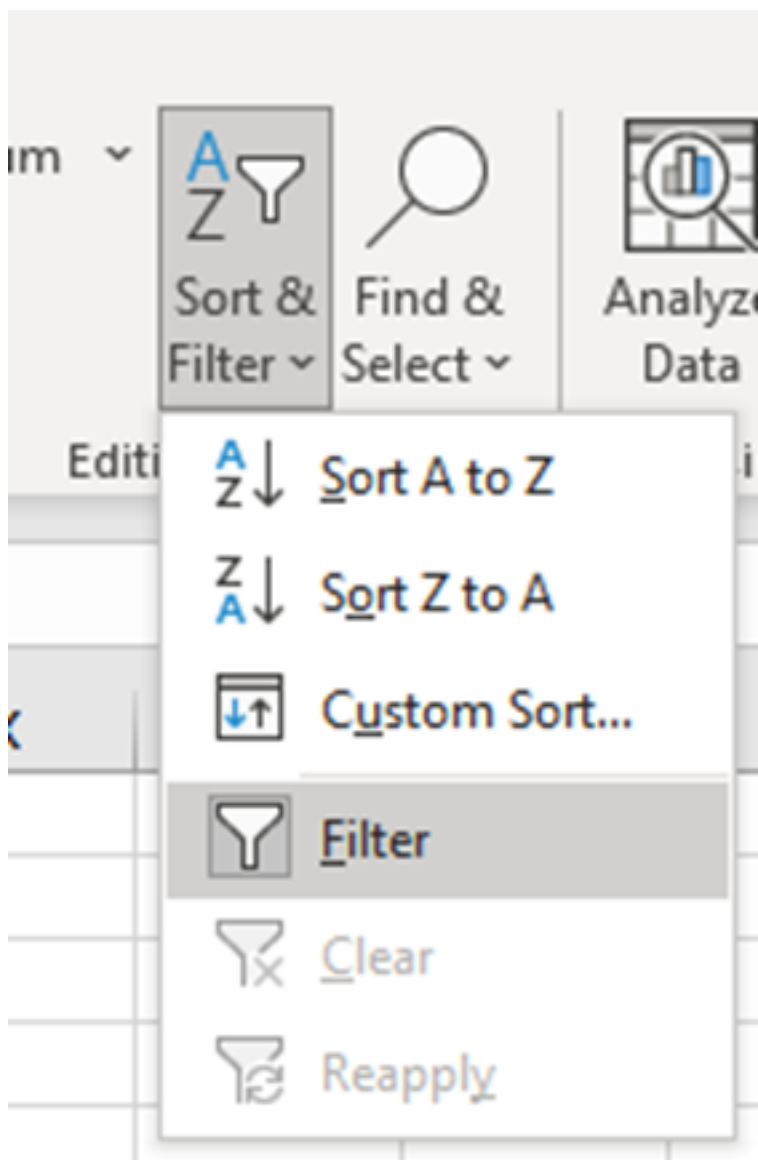
Formula Bar: `=IF(ISNA(VLOOKUP(G2,CAP2_slice!G:G,1,FALSE)),"MISSING","PRESENT")`

	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
	Time	Source	Destinatic Protocol	Length	ESP Sequ	Differenti	Source Po	Destinatic Info	Sequence Number					COMPARE	ESP_SEQUENCE								
51	55.44196	192.168.2.2	192.168.2.2	ESP	176	306	27			ESP (SPI=0x040001dc)				PRESENT									
52	55.44598	192.168.2.2	192.168.2.2	ESP	176	307	27			ESP (SPI=0x040001dc)													
53	55.44897	192.168.2.2	192.168.2.2	ESP	176	308	27			ESP (SPI=0x040001dc)													
54	55.45097	192.168.2.2	192.168.2.2	ESP	176	309	27			ESP (SPI=0x040001dc)													
55	55.45296	192.168.2.2	192.168.2.2	ESP	176	310	27			ESP (SPI=0x040001dc)													
56	55.45496	192.168.2.2	192.168.2.2	ESP	176	311	27			ESP (SPI=0x040001dc)													
57	55.45597	192.168.2.2	192.168.2.2	ESP	176	312	27			ESP (SPI=0x040001dc)													
58	55.45698	192.168.2.2	192.168.2.2	ESP	176	313	27			ESP (SPI=0x040001dc)													
59	55.45797	192.168.2.2	192.168.2.2	ESP	176	314	27			ESP (SPI=0x040001dc)													
50	55.45898	192.168.2.2	192.168.2.2	ESP	176	315	27			ESP (SPI=0x040001dc)													
51	55.46197	192.168.2.2	192.168.2.2	ESP	176	316	27			ESP (SPI=0x040001dc)													
52	55.46397	192.168.2.2	192.168.2.2	ESP	176	317	27			ESP (SPI=0x040001dc)													
53	55.46596	192.168.2.2	192.168.2.2	ESP	176	318	27			ESP (SPI=0x040001dc)													
54	55.46697	192.168.2.2	192.168.2.2	ESP	176	319	27			ESP (SPI=0x040001dc)													
55	55.46796	192.168.2.2	192.168.2.2	ESP	176	320	27			ESP (SPI=0x040001dc)													
56	55.46996	192.168.2.2	192.168.2.2	ESP	176	321	27			ESP (SPI=0x040001dc)													
57	55.47097	192.168.2.2	192.168.2.2	ESP	176	322	27			ESP (SPI=0x040001dc)													
539	55.60297	192.168.2.2	192.168.2.2	ESP	176	324	27			ESP (SPI=0x040001dc)													
540	55.60496	192.168.2.2	192.168.2.2	ESP	176	395	27			ESP (SPI=0x040001dc)													
541	55.60596	192.168.2.2	192.168.2.2	ESP	176	396	27			ESP (SPI=0x040001dc)													
542	55.60696	192.168.2.2	192.168.2.2	ESP	176	397	27			ESP (SPI=0x040001dc)													
543	55.60696	192.168.2.2	192.168.2.2	ESP	176	398	27			ESP (SPI=0x040001dc)													
544	55.60696	192.168.2.2	192.168.2.2	ESP	176	399	27			ESP (SPI=0x040001dc)													
545	55.60796	192.168.2.2	192.168.2.2	ESP	176	400	27			ESP (SPI=0x040001dc)													
546	55.60796	192.168.2.2	192.168.2.2	ESP	176	401	27			ESP (SPI=0x040001dc)													
547	55.60896	192.168.2.2	192.168.2.2	ESP	176	402	27			ESP (SPI=0x040001dc)													
548	55.60896	192.168.2.2	192.168.2.2	ESP	176	403	27			ESP (SPI=0x040001dc)													
549	55.60997	192.168.2.2	192.168.2.2	ESP	176	404	27			ESP (SPI=0x040001dc)													
550	55.61096	192.168.2.2	192.168.2.2	ESP	176	405	27			ESP (SPI=0x040001dc)													

Scroll back to the top of the sheet and click the **COMPARE_ESP_SEQUENCE**. Then select **Sort & Filter**.



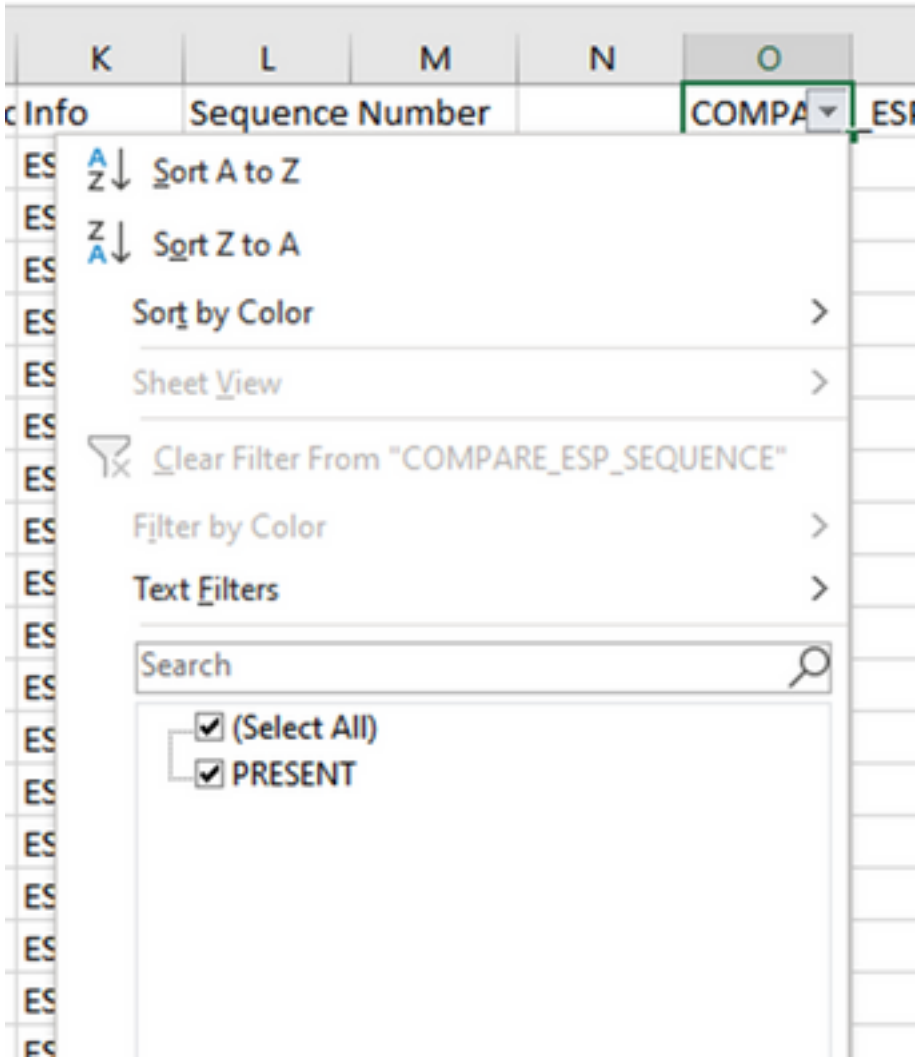
Choose **Filter** from the dropdown menu.



A dropdown menu appears on the **COMPARE_ESP_SEQUENCE** column.

M	N	O	P
Number		COMPARE ESP_SEQUENCE	
		PRESENT	
		PRESENT	
		PRESENT	

Click the dropdown menu on the **COMPARE_ESP_SEQUENCE** heading. Notice that in this example, the only value shown is **PRESENT**. This means all the packets are present in both captures.




To create a problematic example, delete 10 packets from the CAP2_slice, to demonstrate how this would work in a test where some missed packets are missing.


11	472	61.01806	192.168.2:192.168.2	ESP	176	315	27	ESP (SPI=0x040001dc)
12	473	61.01806	192.168.2:192.168.2	ESP	176	316	27	ESP (SPI=0x040001dc)
13	474	61.02106	192.168.2:192.168.2	ESP	176	317	27	ESP (SPI=0x040001dc)
14	475	61.02205	192.168.2:192.168.2	ESP	176	318	27	ESP (SPI=0x040001dc)
15	476	61.02306	192.168.2:192.168.2	ESP	176	319	27	ESP (SPI=0x040001dc)
16	477	61.02506	192.168.2:192.168.2	ESP	176	320	27	ESP (SPI=0x040001dc)
17	478	61.02605	192.168.2:192.168.2	ESP	176	321	27	ESP (SPI=0x040001dc)
18	479	61.02805	192.168.2:192.168.2	ESP	176	322	27	ESP (SPI=0x040001dc)
19	480	61.02906	192.168.2:192.168.2	ESP	176	323	27	ESP (SPI=0x040001dc)
20	481	61.02906	192.168.2:192.168.2	ESP	176	324	27	ESP (SPI=0x040001dc)
21	482	61.03005	192.168.2:192.168.2	ESP	176	325	27	ESP (SPI=0x040001dc)
22	483	61.03206	192.168.2:192.168.2	ESP	176	326	27	ESP (SPI=0x040001dc)
23	484	61.03306	192.168.2:192.168.2	ESP	176	327	27	ESP (SPI=0x040001dc)
24	485	61.03505	192.168.2:192.168.2	ESP	176	328	27	ESP (SPI=0x040001dc)
25	486	61.03606	192.168.2:192.168.2	ESP	176	329	27	ESP (SPI=0x040001dc)
26	487	61.03905	192.168.2:192.168.2	ESP	176	330	27	ESP (SPI=0x040001dc)
27	488	61.04105	192.168.2:192.168.2	ESP	176	331	27	ESP (SPI=0x040001dc)
28	489	61.04206	192.168.2:192.168.2	ESP	176	332	27	ESP (SPI=0x040001dc)
29	490	61.04406	192.168.2:192.168.2	ESP	176	333	27	ESP (SPI=0x040001dc)
30	491	61.04606	192.168.2:192.168.2	ESP	176	334	27	ESP (SPI=0x040001dc)
31	492	61.06305	192.168.2:192.168.2	ESP	176	335	27	ESP (SPI=0x040001dc)
32	493	61.06505	192.168.2:192.168.2	ESP	176	336	27	ESP (SPI=0x040001dc)
33	494	61.06705	192.168.2:192.168.2	ESP	176	337	27	ESP (SPI=0x040001dc)
34	495	61.06905	192.168.2:192.168.2	ESP	176	338	27	ESP (SPI=0x040001dc)
35	496	61.07105	192.168.2:192.168.2	ESP	176	339	27	ESP (SPI=0x040001dc)
36	497	61.07105	192.168.2:192.168.2	ESP	176	340	27	ESP (SPI=0x040001dc)
37	498	61.07205	192.168.2:192.168.2	ESP	176	341	27	ESP (SPI=0x040001dc)
38	499	61.07605	192.168.2:192.168.2	ESP	176	342	27	ESP (SPI=0x040001dc)


Navigate back to **CAP1_slice** sheet and now it is seen that there are 10 packets missing.


Line	Time	Source IP	Destination IP	Protocol	Length	Sequence	Window	Options	Flags	Checksum	Result
460	55.45898	192.168.2.2	192.168.2.2	ESP	176	315	27			ESP (SPI=0x040001dc)	PRESENT
461	55.46197	192.168.2.2	192.168.2.2	ESP	176	316	27			ESP (SPI=0x040001dc)	PRESENT
462	55.46397	192.168.2.2	192.168.2.2	ESP	176	317	27			ESP (SPI=0x040001dc)	PRESENT
463	55.46596	192.168.2.2	192.168.2.2	ESP	176	318	27			ESP (SPI=0x040001dc)	MISSING
464	55.46697	192.168.2.2	192.168.2.2	ESP	176	319	27			ESP (SPI=0x040001dc)	MISSING
465	55.46796	192.168.2.2	192.168.2.2	ESP	176	320	27			ESP (SPI=0x040001dc)	MISSING
466	55.46996	192.168.2.2	192.168.2.2	ESP	176	321	27			ESP (SPI=0x040001dc)	MISSING
467	55.47097	192.168.2.2	192.168.2.2	ESP	176	322	27			ESP (SPI=0x040001dc)	MISSING
468	55.47198	192.168.2.2	192.168.2.2	ESP	176	323	27			ESP (SPI=0x040001dc)	MISSING
469	55.47297	192.168.2.2	192.168.2.2	ESP	176	324	27			ESP (SPI=0x040001dc)	MISSING
470	55.47497	192.168.2.2	192.168.2.2	ESP	176	325	27			ESP (SPI=0x040001dc)	MISSING
471	55.47597	192.168.2.2	192.168.2.2	ESP	176	326	27			ESP (SPI=0x040001dc)	MISSING
472	55.47697	192.168.2.2	192.168.2.2	ESP	176	327	27			ESP (SPI=0x040001dc)	MISSING
473	55.47896	192.168.2.2	192.168.2.2	ESP	176	328	27			ESP (SPI=0x040001dc)	PRESENT
474	55.48096	192.168.2.2	192.168.2.2	ESP	176	329	27			ESP (SPI=0x040001dc)	PRESENT


When the dropdown menu is selected on the **COMPARE_ESP_SEQUENCE** column, now it is seen that there are **MISSING** packets also. This can be toggled to view only the **MISSING** packets.


K	L	M	N	O
Info	Sequence Number			COMPA 


 Sort A to Z


 Sort Z to A


Sort by Color 

Sheet View 

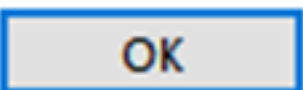
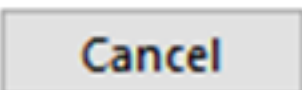
 Clear Filter From "COMPARE_ESP_SEQUENCE"

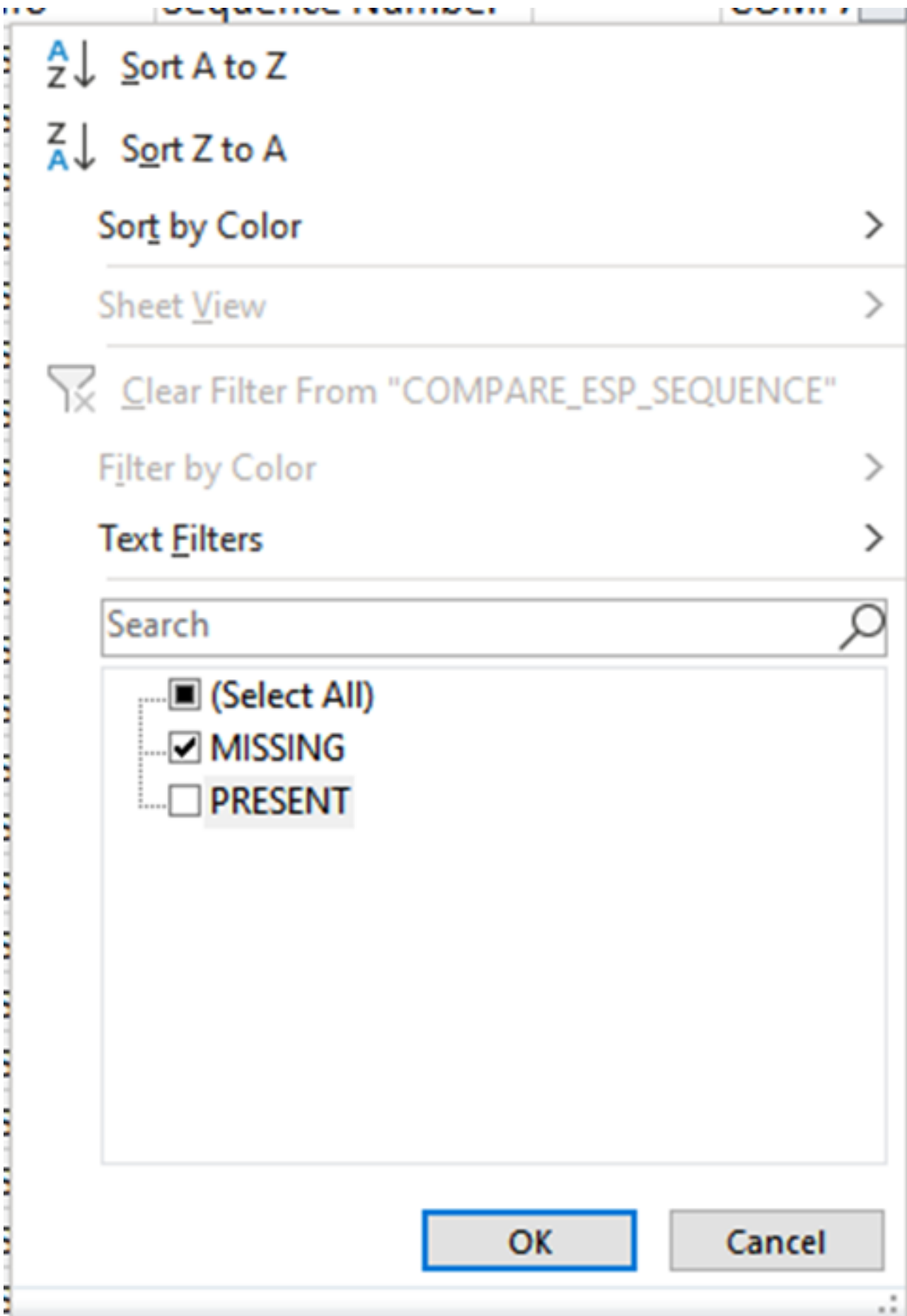
Filter by Color 

Text Filters 

Search 

- (Select All)
- MISSING
- PRESENT



Now only the missing packets are shown in the Excel sheet.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	No.	Time	Source	Destination	Protocol	Length	ESP Sequence	Difference	Source Port	Destination	Info	Sequence Number			COMPACT	ESP_SEQUENCE
4	463	55.46596	192.168.2.2	192.168.2.2	ESP	176	318	27			ESP (SPI=0x040001dc)					MISSING
5	464	55.46697	192.168.2.2	192.168.2.2	ESP	176	319	27			ESP (SPI=0x040001dc)					MISSING
6	465	55.46796	192.168.2.2	192.168.2.2	ESP	176	320	27			ESP (SPI=0x040001dc)					MISSING
7	466	55.46996	192.168.2.2	192.168.2.2	ESP	176	321	27			ESP (SPI=0x040001dc)					MISSING
8	467	55.47097	192.168.2.2	192.168.2.2	ESP	176	322	27			ESP (SPI=0x040001dc)					MISSING
9	468	55.47198	192.168.2.2	192.168.2.2	ESP	176	323	27			ESP (SPI=0x040001dc)					MISSING
0	469	55.47297	192.168.2.2	192.168.2.2	ESP	176	324	27			ESP (SPI=0x040001dc)					MISSING
1	470	55.47497	192.168.2.2	192.168.2.2	ESP	176	325	27			ESP (SPI=0x040001dc)					MISSING
2	471	55.47597	192.168.2.2	192.168.2.2	ESP	176	326	27			ESP (SPI=0x040001dc)					MISSING
3	472	55.47697	192.168.2.2	192.168.2.2	ESP	176	327	27			ESP (SPI=0x040001dc)					MISSING
12																
13																

Related Information

- [Cisco Embedded Packet Capture](#)
- [Technical Support & Documentation - Cisco Systems](#)